Improved practical decoy state method in quantum key distribution with parametric down conversion source

Qin Wang[1], Xiang-Bin Wang[2], Gunnar Björk[1] and Anders Karlsson[1]

[1] *Department of Microelectronics and Information Technology, The Royal Institute of Technology, KTH, Electrum 229, SE-164 40 Kista, Sweden*
[2] *Department of Physics, Tsinghua University, Beijing 100084, China*

PACS. 03.67.Dd – Quantum cryptography.
PACS. 42.65.Lm – Parametric down conversion and production of entangled photons.
PACS. 03.67.Hk – Quantum communication.

Abstract. – In this paper, a new decoy-state scheme for quantum key distribution with parametric down-conversion source is proposed. We use both three-intensity decoy states and their triggered and nontriggered components to estimate the fraction of single-photon counts and quantum bit-error rate of single-photon, and then deduce a more accurate value of key generation rate. The final key rate over transmission distance is simulated, which shows that we can obtain a higher key rate than that of the existing methods, including our own earlier work.

Introduction. – Quantum key distribution has attracted extensive attentions for its unconditional security compared with conversional cryptography [1–6]. However, there still exist several technical limitations in practice, such as imperfect single-photon sources, large loss channels and inefficient detectors, which will impair the security. Fortunately, many methods have been devised to deal with these imperfect conditions [7–12], among which, decoy-state method is thought to be a very useful candidate for substantially improving the performance of QKD.

Decoy-state method was firstly proposed by Hwang [10], and advanced by Wang and Lo *et al.* [11–15] assuming a weak coherent source (WCS). Subsequently, it was extended to parametric down- conversion sources (PDCS) [16–18]. The main idea of decoy-state method is to randomly change the intensity of each pulse among different values, which allows one to estimate the behavior of vacuum, single-photon and multi-photon states individually. As a result, Eve's presence will be detected. Recently, more and more interesting ideas have been put forward to improve the performance of QKD [17, 19, 20], such as the one by Adachi *et al.* [19]. In their proposal, both triggered and nontriggered components of PDCS are used to do some estimations for final secure key, and it needs only one intensity to transmit. However, because the intensity cannot be changed during the whole experiment, and dark counts cannot be measured directly, then the worst case of their contribution must be considered, which will inevitably limit final key rate and transmission distance.

In this paper, we propose a new practical decoy-state scheme with PDCS, in which not only three decoy states with different intensities $(0, \mu, \mu')$, but also all their triggered and nontriggered components are used to estimate the lower bound of fraction of single photon counts (Y_1) and upper bound of quantum bit-error rate (QBER) of single-photon (e_1). As a result, a more accurate value of key generation rate, compared with existing methods, can be obtained.

Improved decoy state method. – In our new scheme, we can essentially use almost the same experimental setup as that in our previous proposal [18], except that Bob's detector need to work no matter what Alice's detector is triggered or not.

As is well known, the state of two-mode field from PDCS is [21, 22]:

$$|\Psi\rangle_{TS} = \sum_{n=0}^{\infty} \sqrt{P_n}\, |n\rangle_T\, |n\rangle_S\,,$$
$$P_n = \frac{x^n}{(1+x)^{n+1}},$$

where $|n\rangle$ represents an n-photon state, and x is the intensity (average photon number) of one mode. Mode T (trigger) is detected by Alice, and mode S (signal) is sent out to Bob. We request Alice to randomly change the intensity of her pump light among three values, so that the intensity of one mode is randomly changed among $0, \mu, \mu'$ (and $\mu < \mu'$).

We denote q_n as the probability of triggering at Alice's detector when an n-photon state is emitted,

$$q_n = 1 - (1-\eta_A)^n\,, \quad n = 1, 2, 3... \tag{1}$$

where η_A is the detecting efficiency at Alice's side, then the nontriggering probability is $(1 - q_n)$. We define Y_n to be the yield of an n-photon state, i.e., the probability that Bob's detector clicks whenever Alice sends out state $|n\rangle$; we also define Q_n be the gain of a n-photon state, i.e., the rate of events when Alice emits n-photon state and Bob detects the signal, which can be divided into two groups, triggered by Alice $Q_n^{(t)}$, and the rest $Q_n^{(ut)}$; and Q_x be the overall rate according to intensity x, (x can be $0, \mu, \mu'$), it can also be divided into two groups, triggered by Alice $Q_x^{(t)}$, and the rest $Q_x^{(ut)}$, which can be expressed as:

$$Q_x^{(t)} = Y_0 \frac{d_A}{1+x} + \sum_{i=1}^{\infty} Y_n \left[1 - (1-\eta_A)^n\right] \frac{x^n}{(1+x)^{n+1}}, \tag{2}$$
$$Q_x^{(ut)} = Y_0 \frac{1-d_A}{1+x} + \sum_{i=1}^{\infty} Y_n \left(1-\eta_A\right)^n \frac{x^n}{(1+x)^{n+1}}, \tag{3}$$

where d_A is the dark count rate of Alice's detector.

In the next step, we will use the triggered events of μ ($Q_\mu^{(t)}$) and the nontriggered events of μ' ($Q_{\mu'}^{(ut)}$) to deduce a tight bound of the fraction of single-photon counts (Y_1).

$$Q_\mu^{(t)} = Y_0 \frac{d_A}{1+\mu} + \sum_{i=1}^{\infty} Y_n \left[1 - (1-\eta_A)^n\right] \frac{\mu^n}{(1+\mu)^{n+1}}, \tag{4}$$
$$Q_{\mu'}^{(ut)} = Y_0 \frac{1-d_A}{1+\mu'} + \sum_{i=1}^{\infty} Y_n \left(1-\eta_A\right)^n \frac{\mu'^n}{(1+\mu')^{n+1}}. \tag{5}$$

The two equations lead to:

$$\begin{aligned}
&\frac{(1+\mu)\left(\frac{\mu'}{1+\mu'}\right)^2 Q_\mu^{(t)}}{1-(1-\eta_A)^2} - \frac{(1+\mu')\left(\frac{\mu}{1+\mu}\right)^2 Q_{\mu'}^{(ut)}}{(1-\eta_A)^2} \\
&= Y_0\left[\frac{\left(\frac{\mu'}{1+\mu'}\right)^2 d_A}{1-(1-\eta_A)^2} - \frac{\left(\frac{\mu}{1+\mu}\right)^2 (1-d_A)}{(1-\eta_A)^2}\right] \\
&+ Y_1\left[\frac{\eta_A}{1-(1-\eta_A)^2}\frac{\mu}{1+\mu}\left(\frac{\mu'}{1+\mu'}\right)^2 - \frac{1}{1-\eta_A}\frac{\mu'}{1+\mu'}\left(\frac{\mu}{1+\mu}\right)^2\right] + \\
&+ \sum_{n=3}^{\infty} Y_n\left[\frac{1-(1-\eta_A)^n}{1-(1-\eta_A)^2}\frac{\mu^n\mu'^2}{(1+\mu)^n(1+\mu')^2} - (1-\eta_A)^{n-2}\frac{\mu'^n\mu^2}{(1+\mu')^n(1+\mu)^2}\right]. \qquad (6)
\end{aligned}$$

Assuming the condition

$$\frac{1-(1-\eta_A)^n}{1-(1-\eta_A)^2}\frac{\mu^n\mu'^2}{(1+\mu)^n(1+\mu')^2} - (1-\eta_A)^{n-2}\frac{\mu'^n\mu^2}{(1+\mu')^n(1+\mu)^2} \leq 0$$

can be satisfied, i.e.

$$\mu \leq \frac{a\mu'}{1+\mu'-a\mu'}, \qquad (7)$$

where $a = \left(\frac{(1-\eta_A)^{n-2}-(1-\eta_A)^n}{1-(1-\eta_A)^n}\right)^{\frac{1}{n-2}}$, (because the values of μ and μ' can be chosen independently, the assumption above can be easily satisfied in experiment,) then Eq. (7) leads to the following inequality:

$$Y_1 \geq Y_1^L = \frac{\frac{(1+\mu)\left(\frac{\mu'}{1+\mu'}\right)^2 Q_\mu^{(t)}}{1-(1-\eta_A)^2} - \frac{(1+\mu')\left(\frac{\mu}{1+\mu}\right)^2 Q_{\mu'}^{(ut)}}{(1-\eta_A)^2} - Y_0\left[\frac{\left(\frac{\mu'}{1+\mu'}\right)^2 d_A}{1-(1-\eta_A)^2} - \frac{\left(\frac{\mu}{1+\mu}\right)^2(1-d_A)}{(1-\eta_A)^2}\right]}{\frac{\eta_A}{1-(1-\eta_A)^2}\frac{\mu}{1+\mu}\left(\frac{\mu'}{1+\mu'}\right)^2 - \frac{1}{1-\eta_A}\frac{\mu'}{1+\mu'}\left(\frac{\mu}{1+\mu}\right)^2}. \qquad (8)$$

This gives rise to the gain of single-photon pulse for triggered and nontriggered components as:

$$Q_1^{(t)}(x) = Y_1\eta_A\frac{x}{(1+x)^2}, \qquad (9)$$

$$Q_1^{(ut)}(x) = Y_1(1-\eta_A)\frac{x}{(1+x)^2}, \qquad (10)$$

and x may be μ or μ' here. Also, if we have observed the quantum bit-error rate (QBER) for triggered and nontriggered pulses of intensity x, $E_x^{(t)}$, $E_x^{(ut)}$, we can upper bound the QBER value of single-photon pulse as:

$$e_1 \leq \frac{(1+x)^2 E_x^{(t)} Q_x^{(t)} - (1+x)Y_0 d_A/2}{Y_1\eta_A x} = e_a, \qquad (11)$$

$$e_1 \leq \frac{(1+x)^2 E_x^{(ut)} Q_x^{(ut)} - (1+x)Y_0(1-d_A)/2}{Y_1(1-\eta_A)x} = e_b, \qquad (12)$$

Combing the two bounds, we have:

$$e_1^U = \min\{e_a, e_b\}\,. \tag{13}$$

Normally, we use the value from $x = \mu$ for a tight estimation of e_1. Given all these, we can use the following formula to calculate the final key-rate of triggered signal pulses [9]:

$$R^{(t)} \geq \frac{1}{2}\left\{-Q_{\mu'}^{(t)} f\left(E_{\mu'}^{(t)}\right) H_2\left(E_{\mu'}^{(t)}\right) + Q_0^{(t)} + Q_1^{(t)}\left[1 - H_2\left(e_1\right)\right]\right\}, \tag{14}$$

where the factor of $\frac{1}{2}$ comes from the cost of basis mismatch in Bennett-Brassard 1984 (BB84) protocol; $f(E_{\mu'})$ is a factor for the cost of error correction given existing error correction systems in practice. We assume $f = 1.22$ here [23]. $H_2\left(x\right)$ is the binary Shannon information function, given by

$$H_2\left(x\right) = -x\log_2(x) - (1-x)\log_2(1-x).$$

Furthermore, if the transmission distance is not so large, the nontriggered component can also be used to generate secret key just as in Adachi *et al*'s proposal [19]:

$$\begin{aligned} R^{(both)} \geq \frac{1}{2}\{&-Q_{\mu'}^{(t)} f\left(E_{\mu'}^{(t)}\right) H_2\left(E_{\mu'}^{(t)}\right) - Q_{\mu'}^{(ut)} f\left(E_{\mu'}^{(ut)}\right) H_2\left(E_{\mu'}^{(ut)}\right) \\ &+ Q_0^{(t)} + Q_0^{(ut)} + \left(Q_1^{(t)} + Q_1^{(t)}\right)\left[1 - H_2\left(e_1\right)\right]\}. \end{aligned} \tag{15}$$

In this case the final key rate is given by: $R = \max\left\{R^{(t)}, R^{(both)}\right\}$.

Numerical simulation. – In an experiment, we need to observe the values of $Q_0^{(t)}$, $Q_\mu^{(t)}$, $Q_{\mu'}^{(t)}$, $Q_0^{(ut)}$, $Q_\mu^{(ut)}$, $Q_{\mu'}^{(ut)}$ and $E_\mu^{(t)}$, $E_{\mu'}^{(t)}$, $E_\mu^{(ut)}$, $E_{\mu'}^{(ut)}$, and then deduce the lower bound of fraction of single-photon counts (Y_1) and upper bound QBER of single-photon pulses (e_1) by theoretical results, and then one can distill the secure final key. In order to make a faithful estimation, we need a channel model to forecast what values for $Q_0^{(t)}$, $Q_\mu^{(t)}$, $Q_{\mu'}^{(t)}$, $Q_0^{(ut)}$, $Q_\mu^{(ut)}$, $Q_{\mu'}^{(ut)}$ and $E_\mu^{(t)}$, $E_{\mu'}^{(t)}$, $E_\mu^{(ut)}$, $E_{\mu'}^{(ut)}$ *would* be, if we *did* the experiment without Eve in principle.

Suppose η is the combined overall transmittance and detection efficiency between Alice and Bob; t_{AB} is the transmittance between Alice and Bob, $t_{AB} = 10^{-\alpha L/10}$; η_B is the transmittance in Bob's side, $\eta = t_{AB}.\eta_B$. Following these assumptions, $Y_n = d_B + 1 - (1-\eta)^n$, which approximates $1-(1-\eta)^n$ when $n \geqslant 1$, and the observed value for $Q_x^{(t)}$ and $Q_x^{(ut)}$ should be:

$$Q_x^{(t)} = \frac{d_A d_B}{1+x} + \sum_{i=1}^{\infty}\left[d_B + 1 - (1-\eta)^n\right]\left[1 - (1-\eta_A)^n\right]\frac{x^n}{(1+x)^{n+1}}, \tag{16}$$

$$Q_x^{(ut)} = \frac{\left(1-d_A\right)d_B}{1+x} + \sum_{i=1}^{\infty}\left[d_B + (1-\eta)^n\right](1-\eta_A)^n\,\frac{x^n}{(1+x)^{n+1}}, \tag{17}$$

where x can be μ or μ', and d_B is the dark count rate of Bob's detectors.

We use the following for the error rate of an *n-photon* state [12]:

$$e_n = \frac{e_0 d_B + e_d[1-(1-\eta)^n]}{d_B + 1 - (1-\eta)^n}, \tag{18}$$

where $e_0 = 1/2$, e_d is the probability that the survived photon hits a wrong detector, which is independent of the transmission distance. Below we shall assume e_d to be a constant.

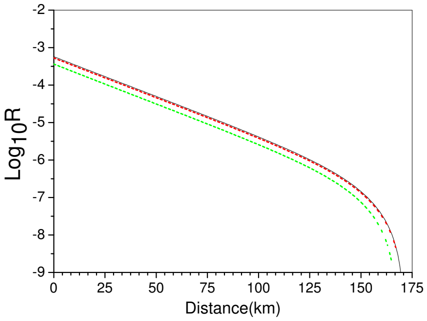

Fig. 1: Fig. 1 (Color online) Final key rates vs transmission distance for decoy-state method. The solid line is the ideal result where the fraction of single-photon counts and QBER of single-photon pulses are known exactly; the dotted lines and dashed lines are the simulation results with finite decoy-state method, among which, the upper line is our new result using only triggered events with $\mu = \frac{a\mu'}{1+\mu'-a\mu'}$; the lower line is the result of our previous proposal with $\mu = 0.1$, (μ' has the optimal value at each point in each line.)

Therefore, the observed $E_x^{(t)}, E_x^{(ut)}$ values should be:

$$E_x^{(t)} = \frac{\sum_{n=0}^{\infty} e_n Q_n^{(t)}(x)}{\sum_{n=0}^{\infty} Q_n^{(t)}(x)}, \tag{19}$$

$$E_x^{(ut)} = \frac{\sum_{n=0}^{\infty} e_n Q_n^{(ut)}(x)}{\sum_{n=0}^{\infty} Q_n^{(ut)}(x)}. \tag{20}$$

In practical implementation of QKD, we often use non-degenerated down-conversion to produce photon pairs [24–26], with one photon at the wavelength convenient for detection acting as heralding signal, and the other at the telecommunication windows for optimal propagation along the fiber or in open air acting as heralded signal. We can now calculate the final key rate with the assumed values above. For convenience of comparing with the results of Adachi *et al.* [19], we use the same parameters as used in their paper which mainly come from Gobby, Yuan and Shields (GYS) experiment [27]. At Alice's side, $d_A = 10^{-6}, \eta_A = 0.5$; at Bob's side, $d_B = 1.7 \times 10^{-6}, \eta_B = 0.045, e_d = 0.033$; and the channel loss is $\alpha = 0.21(dB/km)$. At each distance we choose the optimal value for μ', so that we can have the highest key rate, and the final results are shown in Fig. 1, 2, 3 (according to Eq. (7), $\mu = \frac{a\mu'}{1+\mu'-a\mu'}$ is chosen in our new proposal).

Fig. 1 shows the key generation rate against transmission distance compared with our previous results [18], (only triggered events are used.) It shows that our new scheme can

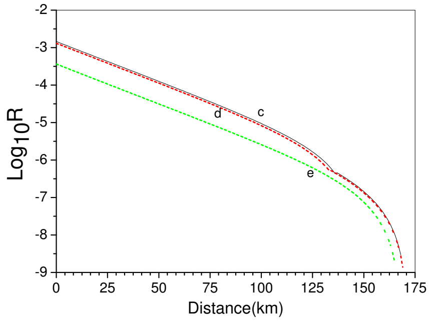

Fig. 2: Fig. 2 (Color online) Final key rates vs transmission distance for decoy-state method. The solid line is the ideal result where the fraction of single-photon counts and QBER of single-photon pulses are known exactly; the dotted lines and dashed lines are the simulation results with finite decoy-state method, among which, the upper line is our new result using both triggered and nontriggered events with $\mu = \frac{a\mu'}{1+\mu'-a\mu'}$; the lower line is the result of our previous proposal with $\mu = 0.1$, (μ' has the optimal value at each point in each line.)

generate a higher key rate than the old one even using only triggered signal.

Fig. 2 shows the key generation rate against transmission distance compared with our previous results [18], (both triggered and nontriggered events are used.) From it we can see that our new results can approach the ideal values very closely. Moreover, there is no need to use a quite weak decoy state or nontriggered signal. For example, at the distance of 50 km, setting $\mu'_{opt} = 0.255, \mu = 0.113, \eta_A = 0.5$ in our new scheme, and $\mu'_{opt} = 0.143, \mu = 0.113, \eta_A = 0.5$ in the old one, we can get a ratio of key rate between the two scheme as 3.8.

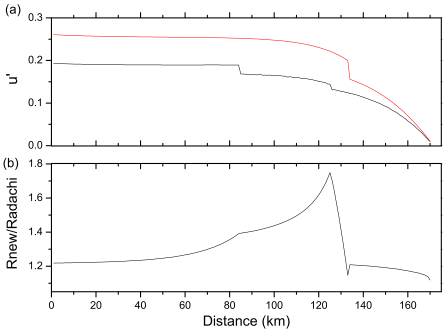

Fig. 3: Fig. 3 (Color online) (a) The optimal value of μ' vs transmission distance. The upper line is the result of our new proposal ($\mu = \frac{a\mu'}{1+\mu'-a\mu'}$), and the lower line is the result of Adachi *et al.* (b) The ratio of key rates between our new proposal and Adachi *et al*'s vs transmission distance.

The reason that we can get a more accurate estimation of key rate (R) in the new proposal is as follows: we don't omit those high order items (in formula (6)) in the deduction of Y_1, but use them to deduce a relationship between the intensity of decoy state (μ) and signal state (μ'), which inevitably results in a more bound estimation of Y_1.(In addition, there is an inflexion in curve c (d) at the distance about 134 km, because the nontriggered events cease to contribute to the key rate.)

Fig. 3 (a) shows the optimal values of μ' in our new proposal (setting $\mu = \frac{a\mu'}{1+\mu'-a\mu'}$) and those in Adachi *et al*'s; Fig. 3 (b) shows the ratio of the key generation rate between our new scheme and Adachi *et al*'s against transmission distance, (both triggered events and nontriggered events are used.) It shows that our result is always larger than theirs when using almost the same level of data size [28].

From the figures above, we can see that, our new results are better than those of both our previous proposal and Adachi *et al*'s. As is known [14], to give a more accurate estimation of the key rate, the value of μ should be chosen to be the smaller the better. In our previous proposal, the key rate could also be very close to the ideal value given a very weak decoy state μ. However, in a practical experiment, considering statistical errors, μ cannot be too weak. So in our new scheme, we deduce a relation between μ and μ', and at each point, both μ and μ' can be chosen with optimal values, which results in a more accurate estimation. Comparing with Adachi *et al*'s proposal, the advantages of our proposal are as follows: Firstly, dark counts can be measured directly; secondly, a weaker decoy state μ is used to get a more accurate estimation of Y_1 and e_1, and a stronger signal of μ' is used to get a higher secure key rate.

Conclusion. – In summary, we have proposed a new decoy-state scheme in QKD with PDCS, in which we use both three-intensity decoy-states and their triggered and nontriggered components to get a tight bound of the fraction of single-photon counts and single-photon QBER, This allows us to accurately deduce the value of key generation rate. Finally, the key generation rate vs transmission distance is numerically simulated. The simulations show that our new results are better than those of the existing proposal. Furthermore, our proposal only assumes existing experimental technology, which makes the scheme a practical candidate in the implementation of QKD.

* * *

Q. W thanks Yoritoshi Adachi (Osaka University) and Sébastien Sauge for useful discussions, and Gao-Xin Qiu for help in numerical simulation. This work was funded by the European Community through the QAP (Qubit Applications-015848) project, and also supported by Chinese National Fundamental Research Program and Tsinghua Bairen Program.

REFERENCES

[1] Bennett C. H. and Brassard G., *in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] Mayers D., *ACM J.* **48** (2001) 351.

[3] Shor P. W. and Preskill J., *Phys. Rev. Lett.* **85** (2000) 441.

[4] Ekert A. K. and Huttner B., *J. Mod. Opt.* **41** (1994) 2455.

[5] Deutsch D. *et al.*, *Phys. Rev. Lett.* **77** (1996) 2818.

[6] Deutsch D. *et al.*, *Phys. Rev. Lett.* **80** (1998) 2022(E).

[7] Scarani V., Acin A., Ribordy G., and Gisin N., *Phys. Rev. Lett.* **92** (2004) 057901; Branciard C., Gisin N., Kraus B., and Scarani V., *Phys. Rev. A* **72** (2005) 032301.

[8] Koashi M., *Phys. Rev. Lett.* **93** (2004) 120501; Tamaki K., Lükenhaus N., Loashi M., and Batuwantudawe J., *New J. Phys.* **8** (2006) 276.

[9] Inamori H., Lütkenhaus N., and Mayers D., e-print quant-ph/0107017; Gottesman D., Lo H. K., Lütkenhaus N., and Preskill J., *Quantum Inf. Comput.* **4** (2004) 325.

[10] Hwang W. Y., *Phys. Rev. Lett.* **91** (2003) 057901.

[11] Wang X. B., *Phys. Rev. Lett.* **94** (2005) 230503.

[12] Lo H. K.,Ma X. , and Chen K., *Phys. Rev. Lett.* **94** (2004) 230504.

[13] Wang X. B., *Phys. Rev. A* **72** (2005) 012322.

[14] Ma X., Qi B., Zhao Y., and Lo H. K., *Phys. Rev. A* **72** (2005) 012326.

[15] Harrington J. W. *et al.*, e-print quant-ph/0503002.

[16] Horikiri T. and Kobayashi T., *Phys. Rev. A* **73** (2006) 032331.

[17] Mauerer W. and Silberhorn C., e-print quant-ph/0609195

[18] Wang Q., Wang X. B., and Guo G. C., *Phys. Rev. A* **75** (2007) 012312.

[19] Adachi Y., Yamamoto T., Koashi M., and Imoto N., e-print quant-ph/0610118.

[20] Qi B., Zhao Y., Ma X., Lo H. K., and Qian L., e-print quant-ph/0611044.

[21] Yurke B. and Potasek M., *Phys. Rev. A* **36** (1987) 3464.

[22] Lütkenhaus N., *Phys. Rev. A* **61** (2000) 052304.

[23] Brassard G. and Salvail L., *Advances in Cryptology EUROCRYPT '93*, Lecture Notes in Computer Science Vol. 765 (Springer, Berlin, 1994), pp. 410–423.

[24] Ljunggren D., Tengner M., Marsden P., and Pelton M., *Phys. Rev. A* **73** (2006) 032326.

[25] Fasel *et al*, *New J. Phys.* **6** (2004) 163.

[26] Mori S., Söderholm J., Namekata N. and Inoue S., *Opt. Comm.* **264** (2006) 156.

[27] Gobby C., Yuan Z. L., and Shields A. *J., Appl. Phys. Lett.* **84** (2004) 3762.

[28] Total photon numbers sent out by Alice in decoy state or in signal state during the whole experiment.